

# PATENT COOPERATION TREATY

From the  
INTERNATIONAL SEARCHING AUTHORITY

To:  
J. WARREN LYTLE, JR.  
SUGHRUE MION, PLLC  
2100 PENNSYLVANIA AVE., NW  
SUITE 800  
WASHINGTON, DC 20037-3123

## PCT

### WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Applicant's or agent's file reference <b>F189122</b>		Date of mailing (day/month/year) <b>21 OCT 2005</b> <b>FOR FURTHER ACTION</b> See paragraph 2 below
International application No. <b>PCT/US04/31728</b>	International filing date (day/month/year) <b>29 September 2004 (29.09.2004)</b>	Priority date (day/month/year) <b>29 September 2003 (29.09.2003)</b>
International Patent Classification (IPC) or both national classification and IPC <b>IPC(7): H04L 9/00 and US Cl.: 713/156</b>		
Applicant <b>AYMAN, LLC</b>		

1. This opinion contains indications relating to the following items:

- ☒ Box No. I      Basis of the opinion
- ☐ Box No. II      Priority
- ☐ Box No. III      Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV      Lack of unity of invention
- ☒ Box No. V      Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI      Certain documents cited
- ☐ Box No. VII      Certain defects in the international application
- ☐ Box No. VIII      Certain observations on the international application

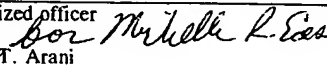
#### 2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Date of completion of this opinion <b>17 September 2005 (17.09.2005)</b>	Authorized officer  Taghi T. Arani Telephone No. (571) 272-3787
--	--	---

Form PCT/ISA/237 (cover sheet) (April 2005)

**WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US04/31728

**Box No. I Basis of this opinion**

1. With regard to the language, this opinion has been established on the basis of:

- ☒ the international application in the language in which it was filed
- ☐ a translation of the international application into \_\_\_\_\_, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any nucleotide and/or amino acid sequence disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

- ☐ a sequence listing
- ☐ table(s) related to the sequence listing

b. format of material

- ☐ on paper
- ☐ in electronic form

c. time of filing/furnishing

- ☐ contained in the international application as filed.
- ☐ filed together with the international application in electronic form.
- ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

**WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY**

International application No.  
PCT/US04/31728

**Box No. V Reasoned statement under Rule 43 bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

**1. Statement**

Novelty (N)	Claims 1-16	YES
	Claims NONE	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-16	NO
Industrial applicability (IA)	Claims 1-16	YES
	Claims NONE	NO

**2. Citations and explanations:**

Claims 1-16 lack inventive step under PCT Article 33(3) as being obvious over Wildish et al. (US 200300115457 A1) in view of Perlman US 2020099668 A1).

Wildish et al teach [Paragraphs 008-00090] a method of establishing a secure communication in a digital communications network having a hierarchical arrangement of a certificate servers, comprising the steps of generating a first private/public key pair in a root certificate server; issuing a digital certificate for a public key portion of said first private/public key pair signed by said root certificate server and identified by a digital identifier associated with said root certificate server; generating additional private/public key pairs in subordinate entities ( certificate-issuing resources) and associating public key portions of said additional private/public key pairs with pseudonymic digital identifiers (i.e. resource identifier containing information identifying each of a plurality of certificate -issuing resources) associated with said respective subordinate entities; and issuing additional digital certificates binding said pseudonymic digital identifiers of said subordinate entities to the public key portion of their respective private/public key pairs from certificate servers (i.e. trusted root) that are in parental relationship to said subordinate entities (certificate -issuing resources) , said additional digital certificates having a digital certificate identifier containing the pseudonymic digital identifier of the certified subordinate entity and the identifier of said certificate server issuing the additional digital certificate.

Wildish et al. further teach (page 1, paragraph 9) the subordinate entities can either be end users or lower level certificate servers and some end users might be certified directly by the root server, whereas other end users would be certified by lower level certificate servers which are themselves certified by higher level servers extending up the chain to the root certificate server.

Wildsidish is silent in disclosing a method of revoking a digital certificate. However, Perlman teach a method and system for revoking a certificate by a certification authority (CA), where an identifier associated with a registration authority (RA) (see Fig. 6, element 56) that requested issuance of a certificate on behalf of a principal is included within the certificate that is issued by the CA (see abstract). The RA contained in the certificate is present on a certification revocation list (CRL) where an indication is sent to the server that a certificate is revoked .

It would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Perlman within the certification system of Wildish et al to efficiently revoke certificates upon recognition that a particular RA (or certificate-issuing resource) has been untrustworthy( Perlman , Page 1, paragraph 0009)

Claims 1-16 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.